BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM17-11-000; Order No. 843]

Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves Critical Infrastructure Protection (CIP) Reliability Standard CIP-003-7 (Cyber Security – Security Management Controls), submitted by the North American Electric Reliability Corporation (NERC). Reliability Standard CIP-003-7 clarifies the obligations pertaining to electronic access control for low impact BES Cyber Systems; requires mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and requires responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. In addition, the Commission directs NERC to develop modifications to the CIP Reliability Standards to mitigate the risk of malicious code that could result from third-party transient electronic devices.

DATES: This rule will become effective **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

FOR FURTHER INFORMATION CONTACT:

Matthew Dale (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6826
matthew.dale@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

Before Commissioners: Kevin J. McIntyre, Chairman;
Cheryl A. LaFleur, Neil Chatterjee,
Robert F. Powelson, and Richard Glick.

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission approves Reliability Standard CIP-003-7 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. Reliability Standard CIP-003-7 addresses the Commission's directives from Order No. 822 and is an improvement over the current Commission-approved CIP Reliability Standards.[2] Specifically, Reliability Standard CIP-003-7 improves upon the existing Reliability Standards by: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems;[3] (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. We also approve NERC's proposed implementation plan and violation risk factor and violation severity level

[1] 16 U.S.C. 824o (2012).

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

[3] BES Cyber System is defined by NERC as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). The acronym BES refers to the bulk electric system. Reliability Standard CIP-002-5.1a (Cyber Security System Categorization) provides a "tiered" approach to cybersecurity requirements, based on classifications of high, medium and low impact BES Cyber Systems.

assignments. Finally, we approve NERC's proposed revised definitions for inclusion in the NERC Glossary.

2. In the NOPR, the Commission proposed to direct that NERC modify Reliability Standard CIP-003-7 to: (1) provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and (2) address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices.[4] The Commission adopts the NOPR proposal regarding third-party transient electronic devices but does not adopt the proposal regarding criteria for electronic access controls for low impact BES Cyber Systems.

3. As discussed below, in view of the comments from NERC and others, we are persuaded that Reliability Standard CIP-003-7 provides a clear security objective that establishes compliance expectations. Accordingly, we do not adopt the proposed directive relating to electronic access controls for low impact BES Cyber Systems. Instead, as suggested in the comments, we direct NERC to conduct a study to assess the implementation of Reliability Standard CIP-003-7 to determine whether the electronic access controls adopted by responsible entities provide adequate security. NERC must submit the directed study within eighteen months of the effective date of Reliability Standard CIP-003-7.

---

[4] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Notice of Proposed Rulemaking, 82 FR 49541 (Oct. 26, 2017), 161 FERC ¶ 61,047 (2017) (NOPR).

4. With regard to the second issue discussed in the NOPR, we remain concerned that the proposed Reliability Standard lacks a clear requirement to mitigate the risk of malicious code that could result from third-party transient electronic devices. Accordingly, we direct NERC to develop a modification to the Reliability Standard to provide the needed clarity. Such modification will better ensure that registered entities clearly understand their mitigation obligations and, thus, improve individual entity mitigation plans and collectively improve the cybersecurity posture of the electric grid.

I. Background

A. Section 215 and Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[5] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[6] and subsequently certified NERC.[7]

---

[5] 16 U.S.C. 824o(e).

[6] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[7] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

B. Order No. 822

6. The Commission approved the "Version 1" CIP Reliability Standards in January 2008, and subsequently acted on revised versions of the CIP Reliability Standards.[8] On January 21, 2016, in Order No. 822, the Commission approved seven CIP Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). The Commission determined that the Reliability Standards under consideration at that time were an improvement over the prior iteration of the CIP Reliability Standards and addressed the directives in Order No. 791 by, among other things, addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks" and providing controls to address the risks posed by transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at high and medium impact BES Cyber Systems.[9]

---

[8] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009); *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[9] Order No. 822, 154 FERC ¶ 61,037 at P 17.

7. In addition, in Order No. 822, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC, *inter alia,* to: (1) develop modifications to the Low Impact External Routable Connectivity (LERC) definition to eliminate ambiguity surrounding the term "direct" as it is used in the LERC definition; and (2) develop modifications to the CIP Reliability Standards to provide mandatory protection for transient electronic devices used at low impact BES Cyber Systems.[10]

C. NERC Petition

8. On March 3, 2017, NERC submitted a petition seeking approval of Reliability Standard CIP-003-7 and the associated violation risk factors and violation severity levels, implementation plan and effective date. NERC states that Reliability Standard CIP-003-7 satisfies the criteria set forth in Order No. 672 that the Commission applies when reviewing a proposed Reliability Standard.[11] NERC also sought approval of revisions to NERC Glossary definitions for the terms Removable Media and Transient Cyber Asset, as well as the retirement of the NERC Glossary definitions of LERC and Low Impact BES Cyber System Access Point (LEAP). In addition, NERC proposed the retirement of Commission-approved Reliability Standard CIP-003-6.[12]

---

[10] *Id.* P 18.

[11] *See* NERC Petition at 2 (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 262, 321-337); *id.*, Exhibit D (Order No. 672 Criteria).

[12] Reliability Standard CIP-003-7 is not attached to this Final Rule. The Reliability Standard is available on the Commission's eLibrary document retrieval system in Docket No. RM17-11-000 and is posted on the NERC website, http://www.nerc.com.

9. NERC states that Reliability Standard CIP-003-7 improves upon the existing protections that apply to low impact BES Cyber Systems. NERC avers that the proposed modifications address the Commission's directives from Order No. 822 by: (1) clarifying electronic access control requirements applicable to low impact BES Cyber Systems; and (2) adding requirements for the protection of transient electronic devices used for low impact BES Cyber Systems. In addition, while not required by Order No. 822, NERC proposes a CIP Exceptional Circumstances policy for low impact BES Cyber Systems.

10. In response to the Commission's directive to develop modifications to eliminate ambiguity surrounding the term "direct" as it is used in the LERC definition, NERC proposes to: (1) retire the terms LERC and LEAP from the NERC Glossary; and (2) modify Section 3 of Attachment 1 to Reliability Standard CIP-003-7 "to more clearly delineate the circumstances under which Responsible Entities must establish access controls for low impact BES Cyber Systems."[13] NERC states that the proposed revisions are designed to simplify the electronic access control requirements associated with low impact BES Cyber Systems to avoid ambiguities associated with the term "direct." NERC explains that it recognized the "added layer of unnecessary complexity" introduced by distinguishing between "direct" and "indirect" access within the LERC

[13] NERC Petition at 16.

definition and asserts that the proposed revisions will "help ensure that Responsible Entities implement the required security controls effectively."[14]

11. With regard to the Commission's directive that NERC develop modifications to the CIP Reliability Standards to provide mandatory protection for transient electronic devices used at low impact BES Cyber Systems, NERC proposes to add a new section to Attachment 1 of Reliability Standard CIP-003-7 that requires responsible entities to include controls in their cyber security plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems that could result from the use of "Transient Cyber Assets or Removable Media." Specifically, proposed Section 5 of Attachment 1 lists controls to be applied to Transient Cyber Assets and Removable Media that NERC contends "will provide enhanced protections against the propagation of malware from transient devices."[15]

12. NERC also proposes a modification that was not directed by the Commission in Order No. 822. Namely, NERC proposes revisions in Requirement R1 of Reliability Standard CIP-003-7 to require responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.[16] NERC states that a number of requirements in the existing CIP Reliability

---

[14] *Id.* at 16.

[15] *Id.* at 26-27.

[16] A CIP Exceptional Circumstance is defined in the NERC Glossary as a situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or bulk electric system reliability: a risk of injury or death; a natural

(continued…)

Standards specify that responsible entities do not have to implement or continue implementing these requirements to avoid hindering the entities' ability to timely and effectively respond to the CIP Exceptional Circumstance. NERC proposes to add a requirement for responsible entities to have a CIP Exceptional Circumstances policy that applies to low impact BES Cyber Systems since the proposed requirements relating to transient electronic devices used at low impact BES Cyber Systems include an exception for CIP Exceptional Circumstances.[17]

13. NERC requests that Reliability Standard CIP-003-7 and the revised definitions of Transient Cyber Asset and Removable Media become effective the first day of the first calendar quarter that is eighteen months after the effective date of the Commission's order approving the Reliability Standard.

D. Notice of Proposed Rulemaking

14. On October 19, 2017, the Commission issued a NOPR that proposed to approve Reliability Standard CIP-003-7. The NOPR proposed to determine that Reliability Standard CIP-003-7 is just, reasonable, not unduly discriminatory or preferential, and in the public interest and addresses the directives in Order No. 822 by: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems;

---

disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

[17] NERC Petition at 31-32.

and (2) adopting mandatory security controls for transient electronic devices used at low impact BES Cyber Systems. In addition, the NOPR observed that, by requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances for low impact BES Cyber Systems, Reliability Standard CIP-003-7 would align the treatment of low impact BES Cyber Systems with that of high and medium impact BES Cyber Systems, which currently include a requirement for declaring and responding to CIP Exceptional Circumstances. Therefore, the Commission proposed to approve Reliability Standard CIP-003-7 because the proposed modifications improve the base-line cybersecurity posture of responsible entities compared to the current Commission-approved CIP Reliability Standards.

15. In addition, the Commission proposed to direct that NERC develop modifications to Reliability Standard CIP-003-7 to addressed two issues: (1) provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and (2) address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices. The Commission explained that modifications directed at these two concerns will address potential gaps and improve the cyber security posture of responsible entities that must comply with the CIP Reliability Standards.

16. The Commission received comments in response to the NOPR from Jonathan Appelbaum (Appelbaum), Electric Consumers Resource Council (ELCON), North American Electric Reliability Corporation (NERC), Transmission Access Policy Study

Group (TAPS), and Trade Associations.[18] We address below the issues raised in the NOPR and comments.

II. Discussion

17. Pursuant to section 215(d)(2) of the FPA, we approve Reliability Standard CIP-003-7 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. Reliability Standard CIP-003-7 addresses the directives in Order No. 822 and is an improvement over the currently-effective, Commission-approved CIP Reliability Standards. Specifically, Reliability Standard CIP-003-7 improves upon the existing CIP Reliability Standards by: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. We also approve NERC's proposed implementation plan and violation risk factor and violation severity level assignments. Finally, we approve NERC's proposed revised definitions for inclusion in the NERC Glossary.

18. In addition, as discussed below, pursuant to section 215(d)(5) of the FPA, we adopt the NOPR proposal and direct NERC to develop modifications to the CIP

[18] Trade Associations represent American Public Power Association, Edison Electric Institute, and National Rural Electric Cooperative Association.

Reliability Standards to mitigate the risk of malicious code that could result from third-party transient electronic devices. However, for the reasons discussed below, we determine not to adopt the NOPR proposal to direct NERC to develop criteria for electronic access controls for low impact BES Cyber Systems at this time.

19. Below, we discuss the following matters: (A) criteria for electronic access controls for low impact BES Cyber Systems; (B) mitigation of the risk of malicious code associated with third-party transient electronic devices; and (C) implementation plan and effective date.

A. Criteria for Electronic Access Controls for Low Impact BES Cyber Systems

1. NOPR

20. In the NOPR, the Commission proposed to direct NERC to develop modifications to Section 3 of Attachment 1 to Reliability Standard CIP-003-7 to provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems.[19] Specifically, the proposed directive addressed the concern that Reliability Standard CIP-003-7 may not provide adequate electronic access controls for low impact BES Cyber Systems because Reliability Standard CIP-003-7 does not provide clear, objective criteria or measures to assess compliance by independently confirming that the access control strategy adopted by a responsible entity would reasonably meet the security objective of permitting only "necessary inbound and outbound electronic access" to its low impact BES Cyber

[19] NOPR, 161 FERC ¶ 61,047 at P 32.

Systems.[20] The Commission stated that, in order to ensure an objective and consistently-applied requirement, the electronic access control plan required in Attachment 1 should require the responsible entity to articulate its access control strategy for a particular set of low impact BES Cyber Systems and provide a technical rationale rooted in security principles explaining how that strategy will reasonably restrict electronic access. In addition, the Commission stated that Attachment 1 should outline basic security principles in order to provide clear, objective criteria or measures to assist in assessing compliance.[21]

21. The Commission observed that without clear, objective criteria or measures, auditors will not necessarily have adequate information to assess the reasonableness of the responsible entity's decision with respect to how the responsible entity identified necessary communications or restricted electronic access to specific low impact BES Cyber Systems. The Commission posited that absent such information, it is possible that an auditor could assess a violation where an entity adequately protected its low impact BES Cyber Systems or fail to recognize a situation where additional protections are necessary to meet the security objective of the Reliability Standard.[22]

2. Comments

[20] *Id.* P 28.

[21] *Id.* P 29.

[22] *Id.*

22. NERC acknowledges the NOPR concerns but comments that a directive "may not be necessary."[23] Specifically, NERC asserts that "Responsible Entities must provide auditors sufficient information to allow the auditors to properly assess compliance with section 3.1" of Reliability Standard CIP-003-7.[24] NERC contends that Section 3.1 "articulates a clear security objective: permit only necessary inbound and outbound access to low impact BES Cyber Systems."[25] NERC explains that Section 3.1 is not prescriptive due to the wide array of low impact BES Cyber Systems and their lower risk to bulk electric system reliability, but, while Section 3.1 grants responsible entities flexibility, "a Responsible Entity must demonstrate that its electronic access permissions and controls are consistent with the security objective."[26] Specifically, NERC maintains that a responsible entity "must document the necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access."[27] NERC states further that "[i]f a Responsible Entity fails to articulate a reasonable business or operational need for the electronic access permission, the ERO Enterprise would find that the Responsible Entity did not comply with Section 3.1."[28] NERC continues that "[c]onsistent with the intent of the Commission's proposed directive, the

[23] NERC Comments at 3.

[24] *Id.* (citing NERC Petition at 21-24).

[25] *Id.*

[26] *Id.* at 3-4.

[27] *Id.* at 4 (citing NERC Petition at 22).

[28] *Id.*

Responsible Entity would have to articulate its access control strategy for the low impact BES Cyber System and provide a technical rationale rooted in security principles, explaining how that strategy will reasonably restrict electronic access."[29] NERC states that if a responsible entity "fails to demonstrate that its chosen electronic access controls are properly designed and implemented to meet the security objective, the ERO Enterprise would find that the Responsible Entity did not comply with Section 3.1" of Reliability Standard CIP-003-7.[30]

23. NERC concludes that while the Commission's proposed directive may not be necessary and could potentially be an inefficient use of NERC and industry resources, "[a]rticulating objective criteria for electronic access controls for low impact BES Cyber Systems may improve clarity and auditability, and help ensure that entities implement effective electronic access controls."[31]

24. Trade Associations, TAPS and ELCON do not support the proposed directive, claiming that the proposal would impose additional burdens on registered entities without a corresponding reliability benefit. Trade Associations and TAPS contend that Section 3 of Attachment 1 to Reliability Standard CIP-003-7 gives responsible entities needed flexibility to develop and implement effective electronic access controls for low impact BES Cyber Systems. TAPS adds that Reliability Standard CIP-003-7 reflects what

---

[29] *Id.*

[30] *Id.*

[31] *Id.* at 5.

NERC, through the standard development process, "determined was a technically appropriate tailoring of electronic access controls requirements to low impact BES cyber systems."[32] Trade Associations recommend, as an alternative to the proposed directive, that the Commission approve the proposed Reliability Standard without modification and monitor its concerns, for example, by directing NERC to conduct a study to assess the implementation by responsible entities of Reliability Standard CIP-003-7 electronic access controls to determine whether there are in fact inadequate controls. According to Trade Associations, a fact-driven assessment would help to inform and demonstrate a reliability and security need for future Commission actions related to the CIP Reliability Standards.[33]

25. Further, Trade Associations assert that a risk-based approach is essential to allow responsible entities to focus their resources on assets that have a higher impact on bulk electric system reliability. ELCON adds that while it "appreciates the value establishing more tangible criteria for adequate Low-Impact BES Cyber System controls, … the additional requirements that the Commission proposes would do nothing to harden a Low-Impact facility against the rapid evolution in cyber warfare."[34]

26. Appelbaum supports the proposed directive regarding Section 3 of Attachment 1 to Reliability Standard CIP-003-7. Appelbaum notes that Reliability Standard CIP-003-7

---

[32] TAPS Comments at 7 (*citing* 16 U.S.C. 824o(d)).

[33] Trade Associations Comments at 9.

[34] ELCON Comments at 4.

"leaves the choice of controls to the [responsible entity] and leaves an Auditor with no requirement basis to perform an audit."[35] Appelbaum states that under "NERC's proposal that each entity establishes their own security plan and only needs to demonstrate compliance and adherence to its plan then … the implementation of security controls will be implemented to various levels of security and differentiated … across the NERC Regions."[36] Appelbaum states further that Reliability Standard CIP-003-7 "will result in different auditor conclusions for similarly situated entities implementing similar protections."[37] Appelbaum concludes that "[c]lear requirements are needed to establish a common understanding of the necessary security to be achieved."[38]

3. Commission Determination

27. We do not to adopt the proposed directive, but rather adopt the Trade Associations' recommendation for a study and report to be filed with the Commission. We are satisfied with the explanation of NERC and other commenters that Section 3 of Attachment 1 to Reliability Standard CIP-003-7 provides a clear security objective that establishes compliance expectations. Specifically, we are persuaded by commenters that Section 3 of Attachment 1 requires responsible entities to adopt security controls to

[35] Applebaum Comments at 5.

[36] *Id.* at 6.

[37] *Id.* at 7.

[38] *Id.*

permit only necessary inbound and outbound electronic access to Cyber Assets connected using a routable protocol to low impact BES Cyber Systems.

28. The concern raised in the NOPR focused on the lack of clear, objective criteria or measures to assess compliance with Reliability Standard CIP-003-7. As noted above, however, NERC states in its comments that responsible entities will be required to demonstrate that electronic access permissions and controls associated with low impact BES Cyber Systems are consistent with the stated security objective. NERC also clarifies that responsible entities will be required to "document the [business or operational] necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access."[39] Given NERC's statements, we believe that there will be adequate measures to assess compliance with Reliability Standard CIP-003-7. We expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective.

29. In response to Appelbaum's comment that auditors will not have a common understanding on which to judge compliance across the ERO enterprise, in view of NERC's comments, we believe that NERC and the Regional Entities will have the ability to assess the effectiveness of a responsible entity's electronic access control plan as well as a responsible entity's adherence to its electronic access control plan.

[39] NERC Comments at 4.

30. Moreover, to ensure that the security controls are implemented and that Section 3 accomplishes its intended purpose, we adopt Trade Associations' proposal and direct NERC to conduct a study to assess the implementation of Reliability Standard CIP-003-7.[40] The study should address what electronic access controls entities choose to implement and under what circumstances, and whether the electronic access controls adopted by responsible entities provide adequate security, as well as other relevant information found by NERC as a result of the study. NERC must file the study within eighteen months of the effective date of Reliability Standard CIP-003-7. We may revisit the need for modifications to Section 3 of Attachment 1 to Reliability Standard CIP-003-7 if warranted by the study determination, or the results of audits or other compliance procedures.

B. Mitigation of the Risk of Malicious Code Associated with Third-Party Transient Electronic Devices

1. NOPR

31. In the NOPR, the Commission proposed to direct NERC to develop modifications to proposed Section 5 of Attachment 1 to Reliability Standard CIP-003-7 to mitigate the risk of malicious code that could result from third-party transient electronic devices.[41] Specifically, the Commission raised a concern that Reliability Standard CIP-003-7 does not explicitly require mitigation of the introduction of malicious code from third-party

[40] Trade Associations Comments at 9.

[41] *Id.* P 41.

managed transient electronic devices, even if the responsible entity determines that the third-party's policies and procedures are inadequate. The Commission noted NERC's statement in its petition that a responsible entity's failure to mitigate this risk "may not constitute compliance."[42] The Commission stated that NERC's explanation suggests that, with regard to low impact BES Cyber Systems, the requirement lacks an obligation for a responsible entity to correct any deficiencies that are discovered during a review of third-party transient electronic device management practices.

32. The Commission expressed concern that Reliability Standard CIP-003-7 may contain a reliability gap where a responsible entity contracts with a third-party but fails to mitigate potential deficiencies discovered in the third-party's malicious code detection and prevention practices prior to a transient electronic device being connected to a low impact BES Cyber System. The Commission explained that the reliability gap would result from the fact that Reliability Standard CIP-003-7 does not contain: (1) a requirement for the responsible entity to mitigate any malicious code found during the third-party review(s); or (2) a requirement that the responsible entity take reasonable steps to mitigate the risks of third party malicious code on its systems, if an arrangement cannot be made for the third-party to do so. The Commission observed that without such

[42] *Id.* P 39 (*citing* NERC Petition at 30).

obligations responsible entities could, without compliance consequences, simply accept the risk of deficient third-party transient electronic device management practices.[43]

33. Therefore, pursuant to section 215(d)(5) of the FPA, the Commission proposed to direct NERC to modify Reliability Standard CIP-003-7 to require responsible entities to implement controls to address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices.

2. Comments

34. NERC states that it "agrees with the Commission that, should a Responsible Entity find that a third party's processes and practices for protecting its transient electronic devices inadequate, the Responsible Entity must be required to take mitigating action prior to connecting third-party transient electronic devices to a low impact BES Cyber System."[44] According to NERC, "failure to take mitigating action in this circumstance[] could result in a finding of noncompliance with Section 5 of Attachment 1."[45] NERC, therefore, asserts that "the proposed directive may not be necessary and may be an inefficient use of NERC and industry resources."[46] NERC observes, however, that

[43] *Id.* P 40 (*citing* Order No. 706, 122 FERC ¶ 61,040 at P 150 (rejecting the concept of acceptance of risk in the CIP Reliability Standards)).

[44] NERC Comments at 6 (citing NERC Petition at 29).

[45] *Id.*

[46] *Id.*

"[m]odifying proposed Section 5 to explicitly include a mitigation requirement for third-part[y] devices may remove any doubt about compliance expectations."[47]

35. Trade Associations and ELCON do not support the proposed directive. Trade Associations contend that "[a]lthough Section 5.2 [of Attachment 1 to CIP-003-7] does not explicitly require the responsible entity to mitigate the introduction of malicious code, risk mitigation is an explicit obligation under Section 5."[48] Trade Associations state that if a responsible entity's plan does not "achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets … then the plan will not comply with Section 5."[49] Trade Associations maintains that the "intent of the requirement is made clear in the Supplemental Material for Section 5 and 5.2, which both require the responsible entities to document how they will mitigate the introduction of malicious code."[50] Trade Associations note in a footnote that:

> Although the Supplemental Material does not create binding obligations on responsible entities, the text of the Supplemental Material in the Proposed Standard further clarifies and reinforces that the binding requirements found in CIP-003-7, Attachment 1, Section 5 include the obligation to take additional steps if a third-party's practices do not meet the security objective.[51]

---

[47] *Id.*

[48] Trade Associations Comments at 10.

[49] *Id.* at 11.

[50] *Id.*

[51] *Id.*

Trade Associations conclude that the Commission should approve Reliability Standard CIP-003-7 without modification.

36. ELCON states that "the requirement for a Low-Impact BES Cyber System owner or operator to actively mitigate deficiencies in third party's anti-virus security programs does exist in [Section 5 of Attachment 1 to Reliability Standard CIP-003-7]."[52] ELCON states that the opening paragraph of Section 5, which requires responsible entities to implement one or more plans to "achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media," establishes an obligation to mitigate any identified deficiencies. ELCON contends that the objective of mitigating the risk "cannot be reached if the Responsible Entity allows a third party to connect an insufficiently evaluated [Transient Cyber Asset] to a Low-Impact BES Cyber System."[53] ELCON argues that the "positioning of the requirement in the opening paragraph of Section 5 assures that mitigating actions must be taken to address deficiencies detected" with responsible entity-owned Transient Cyber Assets, vendor-owned Transient Cyber Assets, and Removable Media.[54]

[52] ELCON Comments at 4 (emphasis in original).

[53] *Id.* at 4-5.

[54] *Id.* at 5.

3. Commission Determination

37. We adopt the NOPR proposal and, pursuant to section 215(d)(5) of the FPA, direct that NERC develop modifications to Reliability Standard CIP-003-7 to address our concern and ensure that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices. NERC could satisfactorily address the identified concern, for example, by modifying Section 5 of Attachment 1 to CIP-003-7 to clarify that responsible entities must implement controls to mitigate the risk of malicious code that could result from the use of third-party transient electronic devices.

38. The directed modification will improve the security posture of responsible entities by clarifying compliance expectations. While commenters claim that the provision is sufficiently clear and ask the Commission not to adopt the proposal, all commenters agree that there is not an explicit requirement to mitigate the threat of malicious code that could result from third-party transient electronic devices. While Trade Associations state that Section 5.2 of Attachment 1 does not explicitly require the mitigation of malicious code, Trade Associations and ELCON suggest that Section 5 generally requires risk mitigation. While commenters agree that, at least implicitly, the mitigation of malicious code is an obligation, the lack of a clear requirement could lead to confusion in both the development of a compliance plan and in the implementation of a compliance plan. In addition, although NERC contends that the proposed directive may not be necessary, NERC agrees that modifying Reliability Standard CIP-003-7 to address the mitigation of malicious code explicitly could clarify compliance obligations.

39. Therefore, pursuant to FPA section 215(d)(5), we direct NERC to develop and submit modifications to Reliability Standard CIP-003-7 to include an explicit requirement that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices.

C. Implementation Plan and Effective Date

NERC Petition

40. In its petition, NERC requests an effective date for Reliability Standard CIP-003-7 and the revised definitions of Transient Cyber Asset and Removable Media on the first day of the first calendar quarter that is eighteen months after the effective date of the Commission's order approving the Reliability Standard. NERC explains that the implementation plan does not alter the previously-approved compliance dates for Reliability Standard CIP-003-6 other than the compliance date for Reliability Standard CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3, which would be replaced with the effective date for Reliability Standard CIP-003-7. NERC also proposes that the retirement of Reliability Standard CIP-003-6 and the associated definitions become effective on the effective date of Reliability Standard CIP-003-7.[55]

41. The NOPR proposed to approve NERC's implementation plan and effective date for Reliability Standard CIP-003-7. The Commission did not receive any comments regarding this aspect of the NOPR. Accordingly, we approve NERC's proposed implementation plan and effective date.

[55] *Id.*, Exhibit C (Implementation Plan).

III. Information Collection Statement

42. The FERC-725B information collection requirements contained in this Final Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[56] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[57] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the Commission's need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

43. The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the proposed revision to CIP Reliability Standard CIP-003-7 as compared to the current Commission-approved Reliability Standard CIP-003-6. The Commission has already addressed the burden of implementing Reliability Standard CIP-003-6.[58] As discussed above, the immediate rulemaking

[56] 44 U.S.C. 3507(d) (2012).

[57] 5 CFR 1320.11 (2017).

[58] *See* Order No. 822, 154 FERC ¶ 61,037 at PP 84-88.

addresses three areas of modification to the CIP Reliability Standards: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.

44. The NERC Compliance Registry, as of September 2017, identifies approximately 1,320 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,100 entities will face an increased paperwork burden under Reliability Standard CIP 003-7, estimating that a majority of these entities will have one or more low impact BES Cyber Systems. Based on these assumptions, we estimate the following reporting burden:

RM17-11-000 Final Rule **(Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards)**

	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[59] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
Create low impact TCA assets plan (one-time)[60]	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000	$1,680
Updates and reviews of low impact TCA assets (ongoing)[61]	1,100	300[62]	330,000	1.5 hrs.[63]; $126	495,000 hrs.; $41,580,000	$37,800
Update/modify documentation to remove LERC and LEAP (one-time)[60]	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000	$1,680

[59] The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for 2016 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Legal (Occupation Code: 23-0000): $143.68

Electrical Engineer (Occupation Code: 17-2071): $68.12

Office and Administrative Support (Occupation Code: 43-0000): $40.89

($143.68 + $68.12 + $40.89) ÷ 3 = $84.23. The figure is rounded to $84.00 for use in calculating wage figures in this NOPR.

[60] This one-time burden applies in Year One only.

[61] This ongoing burden applies in Year 2 and beyond.

[62] We estimate that each entity will perform 25 updates per month. 25 updates *12 months = 300 updates (i.e. responses) per year.

[63] The 1.5 hours of burden per response is comprised of three sub-categories:

Updates to managed low TCA assets: 15 minutes (0.25 hours) per response

Updates to unmanaged low TCA assets: 60 minutes (1 hour) per response

Reviews of low TCA applicable controls: 15 minutes (0.25 hours) per response.

Update paperwork for access control implementation in Section 2[64] and Section 3[65] (ongoing)[61]	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000	$1,680
TOTAL (one-time)[60]			**2,200**		**13,750 hrs.; $3,696,000**	
TOTAL (ongoing)[61]			**331,100**		**501,875 hrs.; $43,428,000**	

45. The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: $3,696,000
- Years 2 and 3: $43,428,000
- The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to policy development, while costs in years 2 and 3 will reflect the

[64] Physical Security Controls.

[65] Electronic Access Controls.

burden associated with maintaining logs and other records to demonstrate ongoing compliance.

46. Title: Mandatory Reliability Standards, Revised Critical Infrastructure Protection Reliability Standards

Action: Revision to FERC-725B information collection.

OMB Control No.: 1902-0248.

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: On Occasion.

Necessity of the Information: This Final Rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves NERC's revised CIP Reliability Standard CIP-003-7 pursuant to section 215(d)(2) of the FPA because it improves upon the currently-effective suite of cyber security CIP Reliability Standards.

Internal Review: The Commission has reviewed the Reliability Standard and made a determination that its action is necessary to implement section 215 of the FPA.

47. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

48. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725

17th Street, NW, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM17-11-000 and OMB Control Number 1902-0248.

IV. Regulatory Flexibility Act Analysis

49. The Regulatory Flexibility Act of 1980 (RFA) generally requires a description and analysis of Final Rules that will have significant economic impact on a substantial number of small entities.[66] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[67] The SBA revised its size standard for electric utilities (effective January 22, 2014) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt hour sales).[68] Reliability Standard CIP-003-7 is expected to impose an additional burden on 1,100 entities[69] (reliability coordinators, generator operators, generator owners,

[66] 5 U.S.C. 601-12 (2012).

[67] 13 CFR 121.101 (2017).

[68] SBA Final Rule on "Small Business Size Standards: Utilities," 78 FR 77343 (Dec. 23, 2013).

[69] Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this Final Rule, we are using a 500 employee threshold due to each affected entity falling within the role of Electric Bulk Power Transmission and Control (NAISC Code: 221121).

interchange coordinators or authorities, transmission operators, balancing authorities, transmission owners, and certain distribution providers).

50. Of the 1,100 affected entities discussed above, we estimate that approximately 857 or 78 percent[70] of the affected entities are small. As discussed above, Reliability Standard CIP-003-7 enhances reliability by providing criteria against which NERC and the Commission can evaluate the sufficiency of an entity's electronic access controls for low impact BES Cyber systems, as well as improved security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems). We estimate that each of the 857 small entities to whom the modifications to Reliability Standard CIP-003-7 applies will incur one-time costs of approximately $3,360 per entity to implement this standard, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $39,480 per year per entity). We do not consider the estimated costs for these 857 small entities to be a significant economic impact.

51. Based on the above analysis, we certify that the approved Reliability Standard will not have a significant economic impact on a substantial number of small entities.

V. Environmental Analysis

52. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect

[70] 77.95 percent.

on the human environment.[71] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[72] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Document Availability

53. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

54. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number of this document, excluding the last three digits, in the docket number field. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online

---

[71] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987).

[72] 18 CFR 380.4(a)(2)(ii) (2017).

Support at (202) 502-6652 (toll free at 1-866-208-3676) or e-mail at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

VII. Effective Date and Congressional Notification

55. The Final Rule is effective [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996. This Final Rule is being submitted to the Senate, House, and Government Accountability Office.

By the Commission.

Issue: April 19, 2018

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2018-08610 Filed: 4/24/2018 8:45 am; Publication Date: 4/25/2018]